日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　６月２４日

出願番号
Application Number:　特願２００２－１８３５１１

[ST.10/C]:　[ＪＰ２００２－１８３５１１]

出願人
Applicant(s):　インターナショナル・ビジネス・マシーンズ・コーポレーション

２００２年１１月１９日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００２－３０９１４９４

【書類名】　特許願

【整理番号】　JP9020102

【提出日】　平成14年 6月24日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C 1/00

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　沼尾　雅之

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　渡邊　裕治

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100106699

【弁理士】

【氏名又は名称】　渡部　弘道

【復代理人】

【識別番号】　100104880

【弁理士】

【氏名又は名称】　古部　次郎

【手数料の表示】

【予納台帳番号】　081504

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0004480

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報配信システム、そのサーバ及び情報処理装置並びにプログラム

【特許請求の範囲】

【請求項１】　所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、

前記鍵管理サーバにアクセスし、前記秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得するユーザ端末と、

前記公開鍵を用いて所定の属性に対する前記属性秘密鍵を持つ前記ユーザ端末が復号可能な暗号化コンテンツを生成するプロバイダ端末とを備え、

前記プロバイダ端末は、前記暗号化コンテンツを配信し、

前記ユーザ端末は、自分の前記属性秘密鍵にて復号可能な前記暗号化コンテンツを復号することを特徴とする情報配信システム。

【請求項２】　前記プロバイダ端末は、前記暗号化コンテンツを受信する前記ユーザ端末を指定せずに前記暗号化コンテンツを配信することを特徴とする請求項１に記載の情報配信システム。

【請求項３】　前記ユーザ端末は、前記鍵管理サーバに対して自分の属性を示す属性値の集合を送信し、

前記鍵管理サーバは、管理している前記秘密鍵のうちで、前記ユーザ端末から送信された属性値に対応する秘密鍵に基づいて、当該ユーザ端末に固有の前記属性秘密鍵を生成し、当該ユーザ端末に送信することを特徴とする請求項１に記載の情報配信システム。

【請求項４】　予め定められた所定の属性値に対する秘密鍵及び公開鍵を格納する鍵格納部と、

所定の属性値の集合を取得し、前記鍵格納部に格納されている前記秘密鍵のうちで、当該属性値に対応する秘密鍵に基づいて、当該属性値の集合に対応する属性秘密鍵を生成する属性秘密鍵生成部と、

ネットワークを介して、所定のユーザ端末から前記属性値の集合を受信すると共に、前記属性秘密鍵生成部にて生成された前記属性秘密鍵を当該ユーザ端末に

送信する送受信部と

を備えることを特徴とするサーバ。

【請求項５】　前記属性秘密鍵生成部は、オブビリアス・トランスファーを実現するプロトコルを用いて前記属性秘密鍵を生成することを特徴とする請求項４に記載のサーバ。

【請求項６】　コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、当該公開鍵を用いて当該公開鍵に対応する秘密鍵で復号される条件鍵を生成する条件鍵生成部と、

前記条件鍵に基づいて前記コンテンツを暗号化する暗号化コンテンツ生成部と、

ネットワークを介して、前記コンテンツの送信先を指定せずに暗号化された前記コンテンツを送信する送信部と

を備えることを特徴とする情報処理装置。

【請求項７】　前記条件鍵生成部は、個々の属性値に対する公開鍵を用いて暗号化された当該属性値に対応する条件鍵を、所定の規則に基づいて組み合わせることにより、前記コンテンツの送信先を制限する条件鍵を生成することを特徴とする請求項６に記載の情報処理装置。

【請求項８】　前記条件鍵生成部は、前記コンテンツを暗号化するためのセッション鍵と当該セッション鍵を復号するための条件鍵とを生成し、

前記暗号化コンテンツ生成部は、前記セッション鍵を用いて前記コンテンツを暗号化することを特徴とする請求項６に記載の情報処理装置。

【請求項９】　ネットワークを介して配信されるコンテンツを受信する情報処理装置において、

所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、当該秘密鍵に基づいて生成され、自装置に関して設定された属性に対応した属性秘密鍵を受信する送受信部と、

暗号化されたコンテンツを取得し、前記属性秘密鍵に基づいて復号する復号処理部と

を備えることを特徴とする情報処理装置。

【請求項１０】　前記送受信部は、自装置に関して設定された属性を示す属性値の集合を前記鍵管理サーバに送信し、当該属性値の集合に基づいて生成された前記属性秘密鍵を当該鍵管理サーバから受信することを特徴とする請求項９に記載の情報処理装置。

【請求項１１】　コンピュータを制御して、所定の公開鍵で暗号化された情報を復号する復号鍵を生成するプログラムであって、

予め定められた所定の属性値に対する秘密鍵及び公開鍵を所定の記憶装置に格納する機能と、

所定の属性値の集合を取得し、前記記憶装置に格納されている前記秘密鍵のうちで、当該属性値に対応する秘密鍵に基づいて、当該属性値の集合に対応する属性秘密鍵を生成する機能と、

ネットワークを介して、所定のユーザ端末から前記属性値の集合を受信すると共に、前記属性秘密鍵を当該ユーザ端末に送信する機能と

を前記コンピュータに実現させることを特徴とするプログラム。

【請求項１２】　前記プログラムにより実現される前記属性秘密鍵を生成する機能は、オブビリアス・トランスファーを実現するプロトコルを用いて前記属性秘密鍵を生成することを特徴とする請求項１１に記載のプログラム。

【請求項１３】　コンピュータを制御して、所定のコンテンツを暗号化し配信するプログラムであって、

コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、当該公開鍵を用いて当該公開鍵に対応する秘密鍵で復号される条件鍵を生成する機能と、

前記条件鍵に基づいて前記コンテンツを暗号化する機能と、

ネットワークを介して、前記コンテンツの送信先を指定せずに暗号化された前記コンテンツを送信する機能と

を前記コンピュータに実現させることを特徴とするプログラム。

【請求項１４】　前記プログラムにより実現される前記条件鍵を生成する機能は、個々の属性値に対する公開鍵を用いて暗号化された当該属性値に対応する条件鍵を、所定の規則に基づいて組み合わせることにより、前記コンテンツの送

信先を制限する条件鍵を生成することを特徴とする請求項１３に記載のプログラム。

【請求項１５】　コンピュータを制御して、ネットワークを介して配信されるコンテンツを受信するプログラムであって、

所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、当該秘密鍵に基づいて生成され、自装置に関して設定された属性に対応した属性秘密鍵を受信する機能と、

暗号化されたコンテンツを取得し、前記属性秘密鍵に基づいて復号する機能とを前記コンピュータに実現させることを特徴とするプログラム。

【請求項１６】　コンピュータを制御して所定の公開鍵で暗号化された情報を復号する復号鍵を生成するプログラムを、当該コンピュータが読み取り可能に格納した記録媒体であって、

前記プログラムは、

予め定められた所定の属性値に対する秘密鍵及び公開鍵を所定の記憶装置に格納する機能と、

所定の属性値の集合を取得し、前記記憶装置に格納されている前記秘密鍵のうちで、当該属性値に対応する秘密鍵に基づいて、当該属性値の集合に対応する属性秘密鍵を生成する機能と、

ネットワークを介して、所定のユーザ端末から前記属性値の集合を受信すると共に、前記属性秘密鍵を当該ユーザ端末に送信する機能と

を前記コンピュータに実現させることを特徴とする記録媒体。

【請求項１７】　コンピュータを制御して所定のコンテンツを暗号化し配信するプログラムを、当該コンピュータが読み取り可能に記録した記録媒体であって、

前記プログラムは、

コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、当該公開鍵を用いて当該公開鍵に対応する秘密鍵で復号される条件鍵を生成する機能と、

前記条件鍵に基づいて前記コンテンツを暗号化する機能と、

ネットワークを介して、前記コンテンツの送信先を指定せずに暗号化された前記コンテンツを送信する機能と

を前記コンピュータに実現させることを特徴とする記録媒体。

【請求項１８】　コンピュータを制御してネットワークを介して配信されるコンテンツを受信するプログラムを、当該コンピュータが読み取り可能に記録した記録媒体であって、

前記プログラムは、

所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、当該秘密鍵に基づいて生成され、自装置に関して設定された属性に対応した属性秘密鍵を受信する機能と、

暗号化されたコンテンツを取得し、前記属性秘密鍵に基づいて復号する機能と

を前記コンピュータに実現させることを特徴とする記録媒体。

【請求項１９】　コンピュータを制御して、所定の公開鍵で暗号化された情報を復号する復号鍵を生成し配布する鍵配布方法において、

ｎ個の秘密鍵及び当該秘密鍵に対応するｎ個の公開鍵を生成し、所定の記憶装置に格納するステップと、

前記記憶装置に格納されたｎ個の秘密鍵のうち、所定のクライアントにより任意に選択されたｋ（≦ｎ）個の秘密鍵に関する情報を取得するステップと、

取得した秘密鍵に関する情報に対応するｋ個の前記秘密鍵を前記記憶装置から読み出し、オブビリアス・トランスファーを実現するプロトコルを用いて、当該ｋ個の秘密鍵に対応するｋ個の前記公開鍵で暗号化された情報を復号する復号鍵を生成するステップと、

生成された前記復号鍵を前記クライアントに提供するステップと

を含むことを特徴とする鍵配布方法。

【請求項２０】　所定の属性値に対する秘密鍵及び公開鍵を管理するサービスプロバイダと、

前記サービスプロバイダにアクセスし、前記秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備え、

所定の前記ユーザ端末は、前記公開鍵を用いて所定の属性に対する前記属性秘

密鍵を持つ前記ユーザ端末が復号可能な暗号化コンテンツを生成して、他のユーザ端末に送信し、

前記他のユーザ端末は、自分の前記属性秘密鍵にて復号可能な前記暗号化コンテンツを復号することを特徴とする情報配信システム。

【請求項２１】　所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、

前記鍵管理サーバにアクセスし、前記秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備え、

所定の前記ユーザ端末は、前記公開鍵を用いて所定の属性に対する前記属性秘密鍵を持つ前記ユーザ端末が復号可能なグループ鍵を生成して他のユーザ端末に送信し、当該グループ鍵により利用が可能となるコンテンツをネットワーク上に設置することを特徴とする情報配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データベース検索システムに関し、特に所定のデータベースが所定のデータを保有しているか否かを検索するシステムに関する。

【０００２】

【従来の技術】

データ通信では、通常、コンテンツの宛先として受信者のアドレスを指定する必要があり、「このような人」というように受信者の属性を指定してコンテンツを送信することはできない。反対に、マルチキャスト（同報通信）の場合、受信者側で送信者（マルチキャストアドレス）を指定してコンテンツを受信することができるが、これも受信者の属性によって受信の可否を指定できるものではない。

【０００３】

今日、パーソナライズされた情報（宣伝）が求められており、個人の属性にあった情報の受け渡しが要求される場面も多い。受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を

満たす人のみが受信できるようなコンテンツ配信システムの実現が望まれている。例えば、条件として〔性別＝男、年齢＝３０歳以上、職業＝会社員、趣味＝旅行〕のようなものが記述でき、予めこの条件を満たすような属性を登録しておいた受信者が、コンテンツを受信できるようなシステムである。

一方、プライバシーの問題も重要であり、個人の属性はまさに保護されるべき情報になっている。

【０００４】

認証およびパーソナライゼーションのための属性管理システムとして代表的なものに、米国マイクロソフト社のPassport［MS Passport］がある。このシステムは、１つのサーバにおいて、口座番号などのユーザの個人情報をすべて管理し、ユーザの承認を前提として、サーバ側にこれを提供しようとするものである。情報は暗号化して送られる。

【０００５】

【発明が解決しようとする課題】

しかし、上述した米国マイクロソフト社のPassportに代表される従来の属性管理システムは、個人情報を全て管理するサーバを前提としているため、利用者は、このサーバ（及びその管理者）を全面的に信頼せざるを得ないという問題がある。すなわち、サーバが不正に個人情報を漏洩しようとする場合、利用者はこれを阻止することができない。

また、セキュリティにおいても、当該サーバのみを攻撃対象とすることができる、すなわちシングルアタックポイントになっているため、たとえ運用上の管理が適切であっても、外部の攻撃によって、個人情報が流出する危険性がある。

【０００６】

そこで、本発明は、受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を満たす人のみが受信できるような情報配信システムにおいて、コンテンツの受け渡しに関わる全ての過程で、個人の属性情報が、送信者も含めた第三者には漏れないようにすることを目的とする。

【０００７】

【課題を解決するための手段】

上記の目的を達成する本発明は、次のように構成されたことを特徴とする情報配信システムとして実現される。この情報配信システムは、所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、この鍵管理サーバにアクセスし、秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得するユーザ端末と、公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末が復号可能な暗号化コンテンツを生成するプロバイダ端末とを備え、このプロバイダ端末は、暗号化コンテンツを配信し、ユーザ端末は、自分の属性秘密鍵にて復号可能な暗号化コンテンツを復号することを特徴とする。

【０００８】

より詳細には、この鍵管理サーバは、予め定められた所定の属性値に対する秘密鍵及び公開鍵を格納する鍵格納部と、所定の属性値の集合を取得し、鍵格納部に格納されている秘密鍵のうちで、この属性値に対応する秘密鍵に基づいて、この属性値の集合に対応する属性秘密鍵を生成する属性秘密鍵生成部と、ネットワークを介して、所定のユーザ端末からこの属性値の集合を受信すると共に、属性秘密鍵生成部にて生成された属性秘密鍵をこのユーザ端末に送信する送受信部とを備える。

【０００９】

また、このプロバイダ端末は、コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、公開鍵を用いて公開鍵に対応する秘密鍵で復号される条件鍵を生成する条件鍵生成部と、条件鍵に基づいてコンテンツを暗号化する暗号化コンテンツ生成部と、ネットワークを介して、コンテンツの送信先を指定せずに暗号化されたコンテンツを送信する送信部とを備える。

ここで、この条件鍵生成部は、個々の属性値に対する公開鍵を用いて暗号化された、この属性値に対応する条件鍵を、所定の規則に基づいて組み合わせることにより、コンテンツの送信先を制限する条件鍵を生成する。

【００１０】

さらに、このユーザ端末は、所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、この秘密鍵に基づいて生成され、自装置に関し

て設定された属性に対応した属性秘密鍵を受信する送受信部と、暗号化されたコンテンツを取得し、属性秘密鍵に基づいて復号する復号処理部とを備える。

ここで、この送受信部は、自装置に関して設定された属性を示す属性値の集合を鍵管理サーバに送信し、この属性値の集合に基づいて生成された属性秘密鍵をこの鍵管理サーバから受信する。

【００１１】

また、本発明は、コンピュータを制御して、上述した鍵管理サーバやプロバイダ端末、ユーザ端末として機能させるプログラムとして実現することができる。このプログラムは、磁気ディスクや光ディスク、半導体メモリ、その他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより、提供することができる。

【００１２】

さらに、本発明は、次のような具体的な情報配信システムとして実現される。すなわち、この情報配信システムは、所定の属性値に対する秘密鍵及び公開鍵を管理するサービスプロバイダと、このサービスプロバイダにアクセスし、この秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備える。そして、所定のユーザ端末は、この公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末が復号可能な暗号化コンテンツを生成して、他のユーザ端末に送信し、かかる他のユーザ端末は、自分の属性秘密鍵にて復号可能な暗号化コンテンツを復号することを特徴とする。

あるいは、本発明による他の情報配信システムは、所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、この鍵管理サーバにアクセスし、この秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備える。そして、所定のユーザ端末は、この公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末が復号可能なグループ鍵を生成して他のユーザ端末に送信し、このグループ鍵により利用が可能となるコンテンツをネットワーク上に設置する。

【００１３】

【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいて、この発明を詳細に説明する。

図１は、本実施の形態による情報配信システムの概略構成を説明する図である。

図１を参照すると、本実施の形態の情報配信システムは、属性の指定に用いられる属性鍵を管理する属性鍵管理サーバ１０と、コンテンツ（情報）の送信者であるプロバイダ端末２０と、コンテンツの受信者であるユーザ端末３０とを備える。

本実施の形態において、属性鍵管理サーバ１０、プロバイダ端末２０及びユーザ端末３０は、ワークステーションやパーソナルコンピュータ、その他のネットワーク機能を備えたコンピュータ装置にて実現される。また、ユーザ端末３０は、ＰＤＡ（personal digital assistants）や携帯電話などのネットワーク機能を備えた情報端末装置にて実現することもできる。

これらの装置は、図示しないネットワークを介してデータ交換を行う。ネットワークの通信回線は有線であると無線であるとを問わない。

【００１４】

図６は、本実施の形態による属性鍵管理サーバ１０、プロバイダ端末２０及びユーザ端末３０を実現するのに好適なコンピュータ装置のハードウェア構成の例を模式的に示した図である。

図６に示すコンピュータ装置は、演算手段であるＣＰＵ（Central Processing Unit：中央処理装置）１０１と、Ｍ／Ｂ（マザーボード）チップセット１０２及びＣＰＵバスを介してＣＰＵ１０１に接続されたメインメモリ１０３と、同じくＭ／Ｂチップセット１０２及びＡＧＰ（Accelerated Graphics Port）を介してＣＰＵ１０１に接続されたビデオカード１０４と、ＰＣＩ（Peripheral Component Interconnect）バスを介してＭ／Ｂチップセット１０２に接続されたハードディスク１０５、ネットワークインターフェイス１０６及びＵＳＢポート１０７と、さらにこのＰＣＩバスからブリッジ回路１０８及びＩＳＡ（Industry Standard Architecture）バスなどの低速なバスを介してＭ／Ｂチップセット１０２に接続されたフロッピーディスクドライブ１０９及びキーボード／マウス１１０とを備える。

なお、図１は本実施の形態を実現するコンピュータ装置のハードウェア構成を例示するに過ぎず、本実施の形態を適用可能であれば、他の種々の構成を取ることができる。例えば、ビデオカード１０４を設ける代わりに、ビデオメモリのみを搭載し、ＣＰＵ１０１にてイメージデータを処理する構成としても良いし、ＡＴＡ（AT Attachment）などのインターフェイスを介してＣＤ－ＲＯＭ（Compact Disc Read Only Memory）やＤＶＤ－ＲＯＭ（Digital Versatile Disc Read Only Memory）のドライブを設けても良い。

【００１５】

図１において、プロバイダ端末２０は、コンテンツの送信先を特定するための属性を指定して、当該コンテンツをユーザ端末３０に送信する。この属性を指定するために属性鍵管理サーバ１０が提供する属性鍵が使用される。属性鍵とは、プロバイダ端末２０からユーザ端末３０への通信において指定し得る属性に対して設定された鍵（秘密鍵及び公開鍵）である。また、ユーザ端末３０は、属性鍵管理サーバ１０から自分の属性に対する属性鍵を取得していれば良く、その数は不特定である。したがって、プロバイダ端末２０は、各ユーザ端末３０に対してマルチキャスト（同報通信）によりコンテンツを送信する。

【００１６】

本実施の形態において、属性および属性の取り得る値（属性値）は、予め決められているものとする。ここで、属性とは、ユーザ端末３０のユーザやユーザ端末３０自体の個性を表す情報であり、本実施の形態が利用されるシステムの態様や運用に応じて種々の情報を属性として定めることができる。また、所定の属性A_iに対して、$V_i=\{v_{i,1}, v_{i,2}, \cdots, v_{i,n}\}$が取り得る値の集合（サイズ$=n_i$）だとする。さらに複数の値を取り得るような属性もあることから、これを一般化してk_i（$\leqq n_i$）個の値を取ることができるものとする。これらは、属性に固有のものとする。例えば、属性A_1が性別だとするとV_1｛男、女｝で$n_1=2$、$k_1=1$となる。

属性条件は、以下のように記述する。ある属性A_iの属性値がv_iであることを$A_i(v_i)$と書く。さらに、ＡＮＤ、ＯＲのオペレータ（演算子）として&、|および括弧（）を使うことにする。例えば、

〔性別＝男、年齢＝３０代、職業＝会社員、趣味＝旅行またはパソコン〕
という属性は、
性別（男）＆年齢（３０代）＆職業（会社員）＆（趣味（旅行）｜趣味（パソコン））
と記述される。

また、以下の説明において、ｐは大きな素数、ｑはｐ－１を割り切るような素数、ｇは有限体Z_p上の位数ｑの元とする。また、特に断らない限り全ての計算はZ_p上で行われるとする。

【００１７】

図２は、本実施の形態における属性鍵管理サーバ１０、プロバイダ端末２０及びユーザ端末３０の構成を示す図である。

図２を参照すると、属性鍵管理サーバ１０は、属性鍵を生成する属性鍵生成部１１と、生成された属性鍵を格納する属性鍵格納部１２とを備える。ここで、属性鍵生成部１１は、属性鍵として予め定められた個々の属性に対する秘密鍵及び公開鍵を生成すると共に、個々のユーザ端末３０との情報のやりとりを通じて当該ユーザ端末３０の個別の属性に対応する秘密鍵（属性秘密鍵）を生成する。生成されたユーザ端末３０に固有の属性秘密鍵は、該当するユーザ端末３０に送られる。

この属性鍵生成部１１は、属性鍵管理サーバ１０を構成するコンピュータ装置におけるプログラム制御されたＣＰＵ１０１にて実現される仮想的なソフトウェアブロックである。属性鍵格納部１２は、属性鍵管理サーバ１０を構成するコンピュータ装置の記憶装置（磁気ディスク装置や光ディスク装置、半導体メモリなど）にて実現される。また、特に図示しないが、属性鍵管理サーバ１０は、プログラム制御されたＣＰＵ１０１及びネットワークインターフェイス１０６にて実現される送受信部を備える。

【００１８】

プロバイダ端末２０は、配信するコンテンツを暗号化する暗号化コンテンツ生成部２１と、暗号化されたコンテンツを復号するために用いられる条件鍵を生成する条件鍵生成部２２とを備える。ここで、暗号化コンテンツ生成部２１は、セ

ッション鍵と呼ばれる共通鍵を用いてコンテンツ自体を暗号化する。これに対し、条件鍵生成部２２は、コンテンツを直接復号する鍵を生成するのではなく、セッション鍵を暗号化し当該セッション鍵を復号するための情報を含む鍵を条件鍵として生成する。

この暗号化コンテンツ生成部２１及び条件鍵生成部２２は、プロバイダ端末２０を構成するコンピュータ装置におけるプログラム制御されたＣＰＵ１０１にて実現される仮想的なソフトウェアブロックである。また、特に図示しないが、プロバイダ端末２０は、プログラム制御されたＣＰＵ１０１及びネットワークインターフェイス１０６にて実現される送受信部を備える。

【００１９】

ユーザ端末３０は、属性鍵管理サーバ１０から取得した当該ユーザ端末３０に固有の属性秘密鍵を保持する属性秘密鍵格納部３１と、属性秘密鍵格納部３１に格納された属性秘密鍵を用いてプロバイダ端末２０から配信された暗号化コンテンツを復号する復号処理部３２とを備える。

属性秘密鍵格納部３１は、ユーザ端末３０を構成するコンピュータ装置や情報端末装置の記憶装置（磁気ディスク装置や光ディスク装置、半導体メモリなど）にて実現される。復号処理部３２は、プログラム制御されたＣＰＵ１０１にて実現される仮想的なソフトウェアブロックである。また、特に図示しないが、ユーザ端末３０は、プログラム制御されたＣＰＵ１０１及びネットワークインターフェイス１０６にて実現される送受信部を備える。

【００２０】

次に、本実施の形態による情報配信システムを実現するために用いられるプロトコルを説明する。

本実施の形態にて用いられるプロトコルは、

１．事前処理としての属性鍵の生成と配布、

２．プロバイダ端末２０による条件鍵の生成、

３．マルチキャストによるコンテンツの配信、

の３つを含む。以下、それぞれについて詳細に説明する。

【００２１】

１．属性鍵生成と鍵配布

属性鍵管理サーバ１０の属性鍵生成部１１は、登録された属性A_iに対する属性値の集合｛$v_{i,1}$，$v_{i,2}$，・・・，$v_{i,n}$｝の各々の値に対して、属性秘密鍵$s_{i,j}$をランダムに選び、さらに属性公開鍵

【数１】

$$y_{i,j} = g^{s_{i,j}} \pmod{p}$$

を公開する。

【００２２】

ユーザ端末３０は、属性鍵管理サーバ１０との間で通信を行い、オブビリアス・トランスファー（Oblivious Transfer：以下、ＯＴと略す）を行うことによって、自分の属性値に対する属性秘密鍵を属性鍵管理サーバ１０にも知られることなく取得する。ここで、ＯＴとは、情報提供者と選択者の２人の間のプロトコルであり、提供者が持つ複数個の情報のうち、いくつかを選択者が選んで得るというものである。この時、以下の２つの条件が満たされなければならない。

（１）選択者のプライバシー：提供者は選択者がどれを選んだかを知ることができない。

（２）提供者のプライバシー：選択者は選んだ情報以外を知ることはできない。

なお、ＯＴについては次の文献に詳細に開示されている。

文献：M. Bellare and S. Micali, Non-interactive oblivious transfer and applications, Advances in Cryptology - Crypto '89, pp. 547-557, 1990.

【００２３】

基本的なＯＴとして1-out-of-2-OTがある。これは、提供者が２つの情報を持ち、選択者はそのうちの１つを選ぶというものである。これを実現する代表的なプロトコルはElGamal暗号を使ったものがある。以下に、このプロトコルを示す。ここで、提供者の持つ情報をI_0、I_1とし、選択者の選択値をb∈｛０，１｝

、～ｂ＝ＮＯＴ　ｂとする。

（１）情報提供者が、乱数ｒを生成し、選択者へ送信。

（２）選択者が、受信した乱数ｒを用いて$K_b = g^x$、$K_{-b} = r / K_b$を生成し、情報提供者へ送信。

（３）情報提供者が、$K_0 * K_1 = r$をチェック。

（４）情報提供者が、暗号化コンテンツ｛E_{I1}，E_{I2}｝を生成し、選択者へ送信。ここで、$E_{I1} = (g^h, I_0 * K_0^h)$、$E_{I2} = (g^h, I_1 * K_1^h)$である。

（５）選択者が、コンテンツI_bを復号。

【００２４】

以上説明した1-out-of-2-OTは、２つの情報の中からいずれか１つを選ぶプロトコルであったが、本実施の形態では、これを拡張してｎ個の情報の中から任意のｋ個の情報を選ぶk-out-of-n-OTを実行する。このプロトコルについて、図３を参照して詳細に説明する。

属性A_iの属性値数がｎで、選択可能数がｋであるものとする。

（１）属性鍵管理サーバ１０は、予め秘密の値t_0を決め、

【数２】

$$Q_0 = g^{t_0} \pmod p$$

を公開しておく。

（２）ユーザ端末３０は、ｋ個の秘密鍵｛t_1，t_2，・・・，t_k｝をランダムに決め、その公開鍵

【数３】

$$Q_i = g^{t_i} \pmod p$$

を計算する。ｎ個の属性値の集合｛$v_{i,1}$，$v_{i,2}$，・・・，$v_{i,n}$｝の中から選び出したｋ個の集合｛$v_{i,h(1)}$，$v_{i,h(2)}$，・・・，$v_{i,h(k)}$｝が自分の属性だとする。ｋ＋１個の点｛（０，Ｑ０），（ｈ（１），Ｑ１），・・・，（ｈ（ｋ

），Ｑｋ）｝を通るようなｋ次多項式Ｙ（ｘ）は、ラグランジュの補間法を使えば一意に決められる。この多項式を使ってｎ個の点｛Ｙ（１），Ｙ（２），・・・，Ｙ（ｎ）｝を属性鍵管理サーバ１０に送信する（秘密通信路を用いる必要はない）。

（３）属性鍵管理サーバ１０の属性鍵生成部１１は、ユーザ端末３０の公開している（ユーザ端末３０から送信された）ｎ個の点がｋ次多項式上の点であることを以下の方法で検証した後、正しくｋ次多項式上の点であるならば、Ｙ（ｊ）をそれぞれＥｌＧａｍａｌ暗号の公開鍵として、属性秘密鍵s_{ij}を暗号化したものをユーザ端末３０に送信する（秘密通信路を用いる必要はない）。

（ｎ点がｋ次多項式上の点であることの検証）

「ｎ個の点集合U_1，・・・，U_nからｋ＋１個の点をランダムに選んだ２つの集合S_1とS_2を$S_1 \cup S_2 = U_n$になるように作る。それぞれのセットからｋ次多項式を構成し、それらが等しいことを検証する。」

（４）ユーザ端末３０は、属性鍵管理サーバ１０から受信した、暗号化された属性秘密鍵s_{ij}を用いて、ｈ（ｊ）（$1 \leqq j \leqq k$）によって指定されたｋ個の点のＥｌＧａｍａｌ暗号文のみを復号できる。すなわち、ｋ個の属性秘密鍵を得ることができた。

【００２５】

また、数値属性に対する属性秘密鍵は、上記のk-out-of-n-OTとは別に、次のような表現を用いて生成される。

（１）ｎビットの正整数ｘのバイナリ表現を（x_{n-1}，・・・，x_0）とする。

（２）属性鍵管理サーバ１０の属性鍵生成部１１は、２ｎ組の秘密鍵・公開鍵のペア｛（$pk_j^{(0)}$，$sk_j^{(0)}$），（$pk_j^{(1)}$，$sk_j^{(1)}$）｝（ｊ＝０，．．，ｎ－１）を生成し、各桁に対して、２種類の秘密鍵を割り当てる。すなわち、ｊ桁目に対して、$sk_j^{(0)}$と$sk_j^{(1)}$を割り当てる。これに対応する公開鍵$pk_j^{(0)}$，$pk_j^{(1)}$は公開する。

（３）既存の手法である1-out-of-2 OTによる属性鍵配布により、値Ｘ＝（x_{n-1}，・・・，x_0）を選択したユーザ端末３０は、（$sk_j^{(xn-1)}$，・・・，$sk_j^{(x0)}$）を取得する。

【００２６】

以上のように、k-out-of-n-OTや、数値属性に対して1-out-of-2 OTを用いて属性秘密鍵を配布することにより、ユーザ端末３０は、自分の属性（ｋの値）を属性鍵管理サーバ１０にも知られることなく、すなわち個人情報を全く漏らすことなく、当該自分の属性に対応する属性秘密鍵を取得することができる。

【００２７】

２．条件鍵の生成

プロバイダ端末２０の条件鍵生成部２２は、属性鍵管理サーバ１０が公開している属性公開鍵を次に示すように組み合わせることによって、条件鍵を生成する。なお、Ｅ（ＰＫ、Ｋ）は、公開鍵ＰＫでセッション鍵Ｋを暗号化することを示す。

（１）ＡＮＤ鍵の構成：属性条件A_i（v_{ij}）＆A_k（v_{kl}）に対しては、それぞれ属性公開鍵y_{ij}、y_{kl}が対応している。２つのセッション鍵K_{ij}、K_{kl}をランダムに選び、これを公開鍵でそれぞれ暗号化すると条件鍵は｛E（y_{ij}，K_{ij}），E（y_{kl}，K_{kl}）｝となり、対応するセッション鍵は$K=K_{ij}+K_{kl}$になる。この他、E（y_{ij}，E（y_{kl}，K））もＡＮＤを構成する暗号化になる。

（２）ＯＲ鍵の構成：属性条件A_i（v_{ij}）｜A_k（v_{kl}）に対しては、それぞれ属性公開鍵y_{ij}、y_{kl}が対応している。セッション鍵Ｋの１つをランダムに選び、これを２つの公開鍵で暗号化する。条件鍵は｛E（y_{ij}，K），E（y_{kl}，K））｝となる。

（３）ＮＯＴ鍵の構成：属性条件＾A_i（v_{ij}）に対しては、属性公開鍵y_{ik}、$k=1$、・・・、$j-1$、$j+1$、・・・、n_iが対応している。セッション鍵Ｋを１つランダムに選び、これをn_i-1つの公開鍵で暗号化する。条件鍵はE（y_{i1}，K）||・・・||E（y_{ij-1}，K）||E（y_{ij+1}，K）||・・・||E（y_{ini}，K）となる。

（４）ＡＮＤ／ＯＲの複合条件：上記を最下位レベルのオペレータから繰り返して、条件鍵をコンカテネートし、セッション鍵を計算していけば、任意のＡＮＤ、ＯＲの組み合わせに対する条件鍵およびセッション鍵を作ることができる。

【００２８】

また、所定のｎビットの正整数Ｙ＝（y_{n-1}，・・・，y_0）に関して、Ｘ＞Ｙが成立する場合にのみコンテンツを復号可能としたい場合を考える。プロバイダ端末２０の条件鍵生成部２２は、Ｃ＝（c_{n-1}，・・・，c_0）を以下のようにして計算する。ここで、k_{n-1}，・・・，k_0は乱数とし、k_0＝Ｋを数値属性条件（Ｘ≧Ｙ）に対するセッション鍵とする。次に、c_{n-1}，・・・，c_0を、以下のようにして決める。

$c_j = E(sk^{(1)}_j, k_j)$ if $y_j = 1$

$c_j = E(sk^{(0)}_j, K) || E(sk^{(1)}_j, k_j)$ if $y_j = 0$

プロバイダ端末２０は、（c_{n-1}，$E_{kn-1}(c_{n-2})$，・・・，$E_{k1}(c_0)$）を条件鍵としてユーザ端末３０へ送る。ユーザ端末３０は、Ｘ≧Ｙであれば、Ｋが求まる。

同様の手法により、Ｘ＞Ｙ、Ｘ≦Ｙ、Ｘ＜Ｙについても条件鍵を生成することができる。また、この手法による数値属性条件を組み合わせることにより、Ｙ≦Ｘ≦Ｙ'のような条件鍵を生成することもできる。

図４は、以上のプロトコルを説明する図である。

【００２９】

３．マルチキャストによる配信

プロバイダ端末２０は、上記の条件鍵生成プロトコルにて生成した条件鍵をコンテンツヘッダに付し、同じく上記条件鍵生成プロトコルにて生成したセッション鍵でコンテンツ本体を暗号化した上で、当該コンテンツヘッダ付きの暗号化コンテンツをマルチキャストする。図５は、このマルチキャストの様子を説明する図である。マルチキャストされたコンテンツは、条件鍵の条件に適合する属性秘密鍵を持つユーザ端末３０だけが復号することができる。

【００３０】

以上説明のように構成された本実施の形態による情報配信システムは、次に示すような大きな特徴を有する。

（１）効率性および鍵取得のオフライン性：

ユーザ端末３０は、属性鍵管理サーバ１０から属性秘密鍵を受け取るが、これは１ラウンドのプロトコルで実現される。また、事前に一度、鍵取得をしておけ

ば、その後のマルチキャストに何回でも利用可能である。

（２）プロバイダ端末２０の登録不要：

プロバイダ端末２０は、属性鍵管理サーバ１０の属性公開鍵を利用するが、この時、属性鍵管理サーバ１０との対話は必要ない。また、属性公開鍵は再利用可能である。

（３）属性鍵管理サーバ１０のオフライン性：

属性鍵管理サーバ１０は、ユーザ端末３０の鍵取得時だけに関わり、実際の通信には関わらない。したがって、実際の通信では、ＩＰマルチキャストなどの一般的なマルチキャストあるいはブロードキャストのプロトコルを使うことができる。

（４）受信グループのオープン性：

マルチキャストによって、プロバイダ端末２０は、受信者グループ及び受信可能な全体集合を知ることなく送信ができる。逆に言えば、ユーザ端末３０は、任意の時間に属性鍵管理サーバ１０から属性秘密鍵を受け取ることによって、受信可能グループに参加することができる。

【００３１】

次に、本実施の形態を適用可能な情報配信システムの具体例を説明する。

１：パーソナライズされた電子メール配信サービス

サービスプロバイダを介して複数のあるいは不特定のユーザに対して電子メールを配信するシステムがある。かかるシステムにおいて、サービスプロバイダ７００が属性鍵管理サーバ１０を運営し、電子メールの送信者７１０がプロバイダ端末２０として、所定の属性に対応した条件鍵に基づいて暗号化された電子メールを配信することができる。図７に、かかるシステムの概略構成を示す。

本実施の形態によれば、電子メールの送信者は、電子メールの受信者の属性を特定するが、誰が特定された属性を持つかを知ることはできないため、各ユーザの属性に関するプライバシーは完全に守られる。そのため、ユーザは安全に自分の属性に対する秘密鍵を取得し、パーソナライズされた情報を受け取ることができる。このシステムは、従来のデータベースマーケティングが，送信者側の類推によって受信者を選別していたモデルと異なり、受信者が自分の欲しい情報を能

動的に取ることができるため、よりヒット率の高い配信が可能になることが期待できる。

【００３２】

２：分散マッチングサービスシステム

サービスプロバイダを介して複数のあるいは不特定のユーザ間で情報を照会し、交換するサービスがある。例えば、ネットワークを介したお見合サービスなどである。お見合サービスでは、会員であるユーザ間で交際条件及び自分のプロフィール情報を交換し、交換した情報に基づいて交際相手を捜すことが行われる。この場合、サービスプロバイダ８００が属性鍵管理サーバ１０を運営し、各ユーザの端末８１０がプロバイダ端末２０及びユーザ端末３０として機能する。そして、交換しようとする交際条件やプロフィール情報の項目を属性として指定し、当該属性に対応した条件鍵に基づいて暗号化されたメッセージをやり取りすることにより、互いの交換情報以外の情報を完全に秘匿したまま、情報交換を行うことが可能となる。図８に、かかるシステムの概略構成を示す。

【００３３】

３：分散検索サービスシステム

検索エンジンの運営者が属性鍵管理サーバ１０を運営し、属性として、専門分野などをキーワードとして登録しておく。ユーザ端末３０は、自分の専門分野の属性秘密鍵を取得しておく。プロバイダ端末２０に相当する質問者９１０が、質問をキーワードの組み合わせの形で設定し、ネットワークを介して配信する。すると、所定のユーザ端末３０は、自分の専門に適合するときだけ、その質問を復号して見ることができ、質問に対する返答を行うことができる。図９にかかるシステムの概略構成を示す。

【００３４】

４：コミュニティ鍵生成方式

図１０に、本実施の形態による情報配信システムを用いたコミュニティ鍵生成法式の概略構成を示す。ＩＳＰ（Internet Service Provider）などのネットワーク運営者が属性鍵管理サーバ１０を運営する。そして、コミュニティのトピックを属性として登録しておく。コミュニティの会員は、プロバイダ端末２０及び

ユーザ端末３０として機能する端末装置１０１０を使用する。そして、ユーザ端末３０としての機能により、自分の関心のあるトピックに対する属性秘密鍵を取得しておく。所定の会員は、自由に属性条件を組み合わせて、チャットルーム１０２０を開き、そのグループ鍵をメッセージとして生成し、当該属性条件に対応した条件鍵に基づき暗号化し、他の会員に配信する。これにより、当該属性条件に適合する受信者だけがグループ鍵を復号し、チャットルーム１０２０に参加できることとなる。なお、チャットルーム以外にも、ネットワーク上に置かれた種々のコンテンツを取得する鍵として条件鍵及び属性秘密鍵を設定できることは言うまでもない。

【００３５】

【発明の効果】

以上説明したように、本発明によれば、受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を満たす人のみが受信できるような情報配信システムにおいて、コンテンツの受け渡しに関わる全ての過程で、個人の属性情報が、送信者も含めた第三者に漏れないようにすることができる。

【図面の簡単な説明】

【図１】　本実施の形態による情報配信システムの概略構成を説明する図である。

【図２】　本実施の形態における属性鍵管理サーバ、プロバイダ端末及びユーザ端末の構成を示す図である。

【図３】　本実施の形態によるk-out-of-n-OTによる属性秘密鍵の配布プロトコルを説明する図である。

【図４】　本実施の形態による条件鍵生成プロトコルを説明する図である。

【図５】　本実施の形態によるコンテンツの配信の様子を示す図である。

【図６】　本実施の形態による属性鍵管理サーバ、プロバイダ端末及びユーザ端末を実現するのに好適なコンピュータ装置のハードウェア構成の例を模式的に示した図である。

【図７】　パーソナライズされた電子メール配信サービスシステムに本実施

の形態の情報配信システムを適用した構成を示す図である。

【図８】　分散マッチングサービスシステムに本実施の形態の情報配信システムを適用した構成を示す図である。

【図９】　分散検索に本実施の形態の情報配信システムを適用した構成を示す図である。

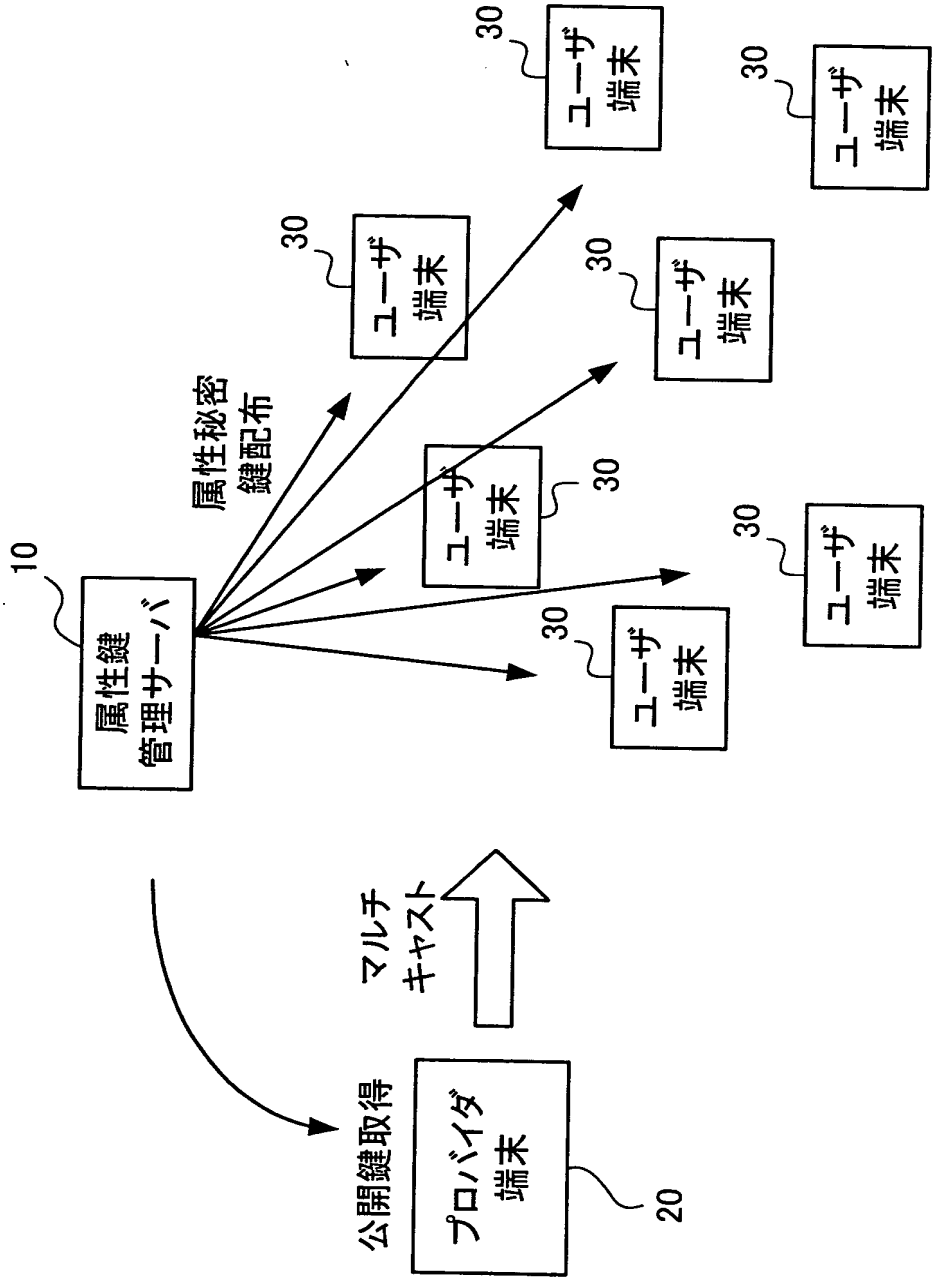
【図１０】　本実施の形態による情報配信システムを用いたコミュニティ鍵生成法式の概略構成を示すである。

【符号の説明】

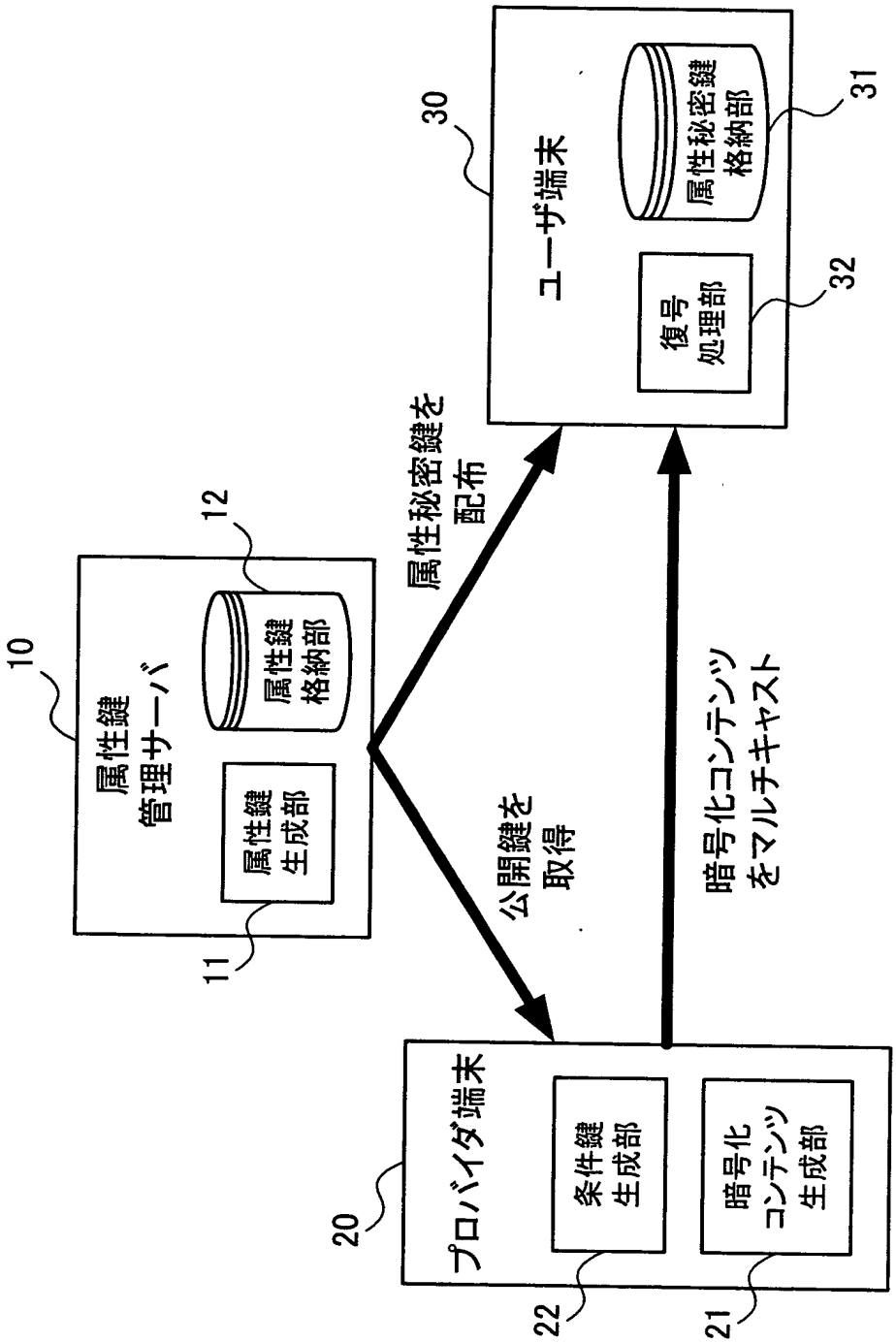
１０…属性鍵管理サーバ、１１…属性鍵生成部、１２…属性鍵格納部、２０…プロバイダ端末、２１…暗号化コンテンツ生成部、２２…条件鍵生成部、３０…ユーザ端末、３１…属性秘密鍵格納部、３２…復号処理部

【書類名】　図面

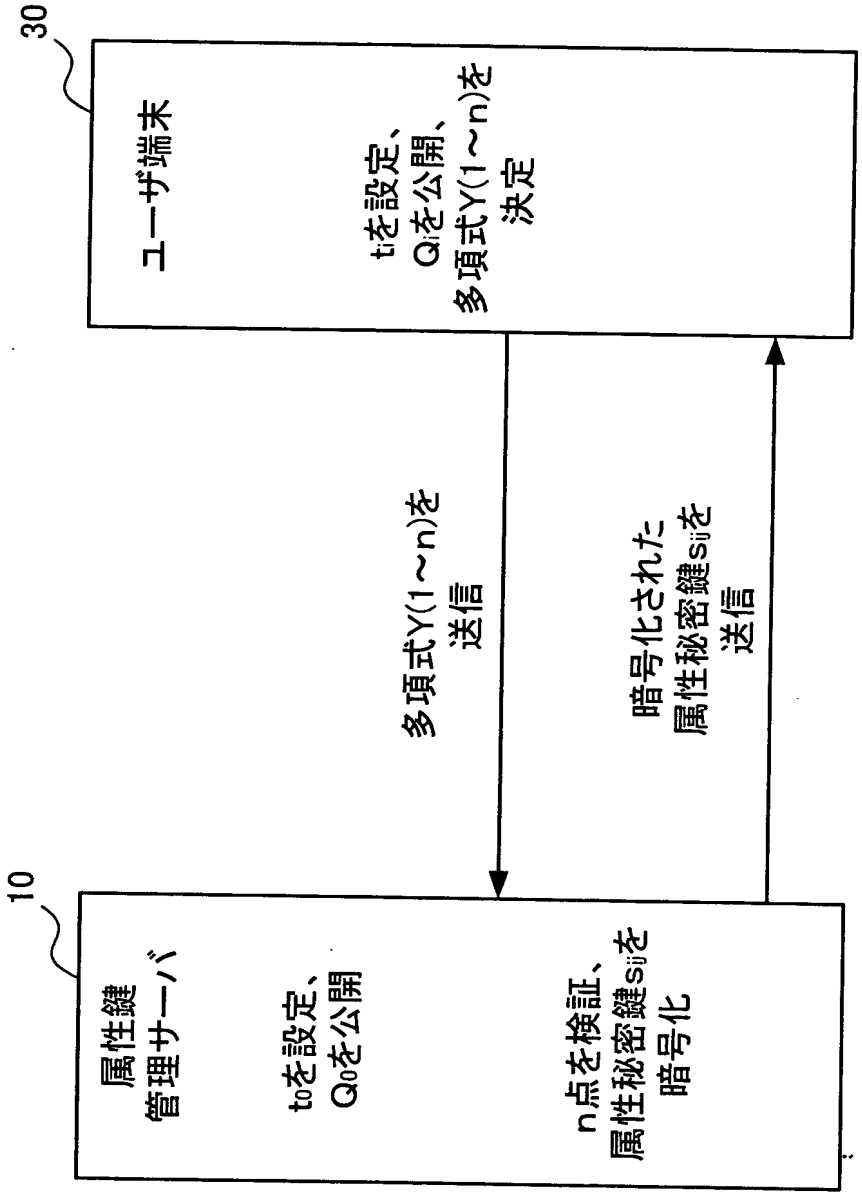
【図１】



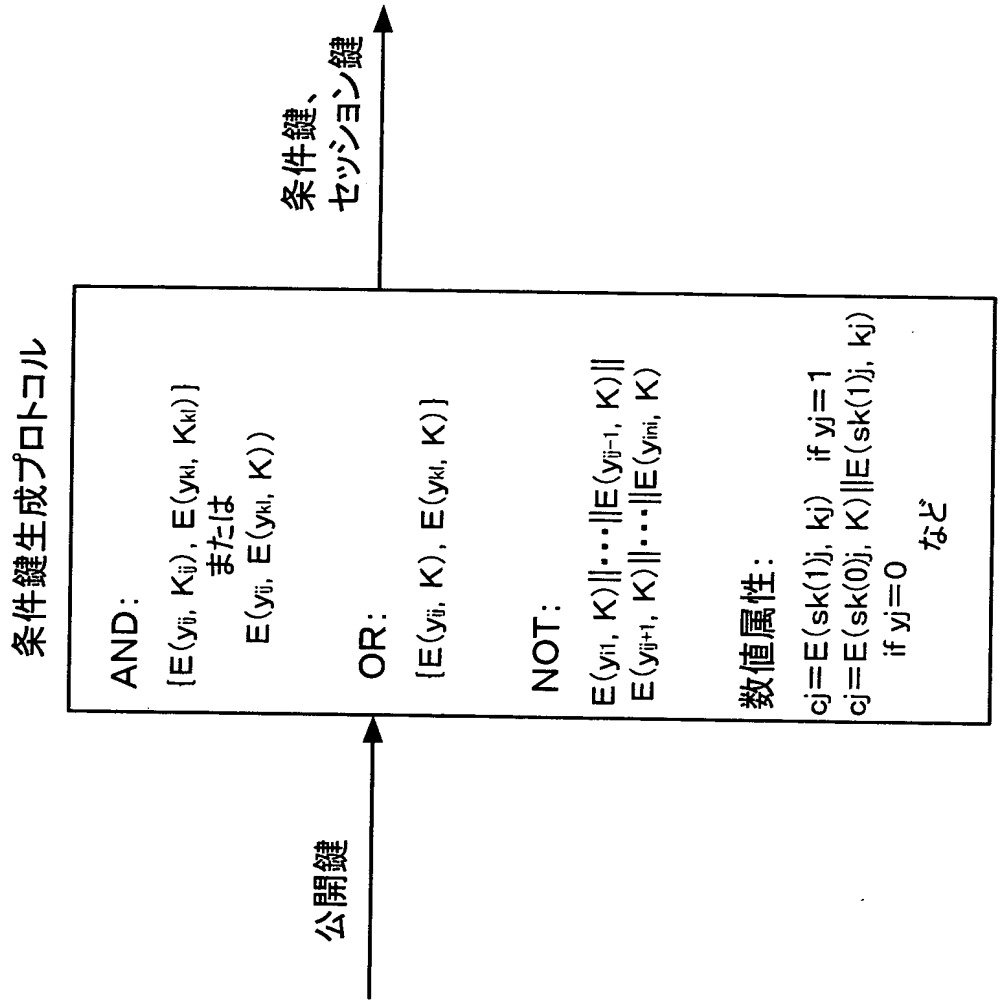
【図２】


10
属性鍵
管理サーバ
12
属性鍵
格納部
属性鍵
生成部
11
属性秘密鍵を
配布
公開鍵を
取得
30
ユーザ端末
属性秘密鍵
格納部
31
復号
処理部
32
暗号化コンテンツ
をマルチキャスト
20
プロバイダ端末
条件鍵
生成部
22
暗号化
コンテンツ
生成部
21

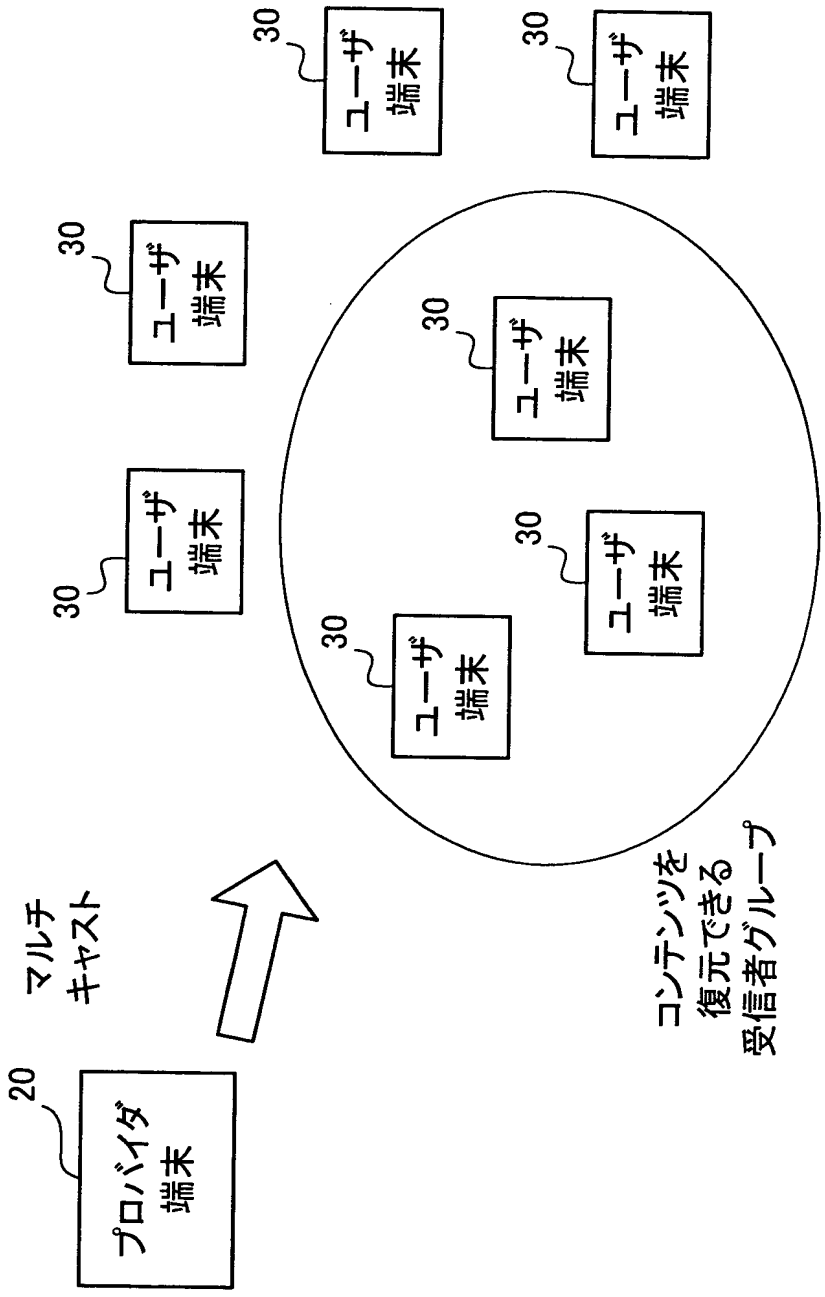
【図３】


30
ユーザ端末
t_iを設定、
Q_iを公開、
多項式Y(1～n)を
決定
多項式Y(1～n)を
送信
暗号化された
属性秘密鍵s_{ij}を
送信
10
属性鍵
管理サーバ
t_0を設定、
Q_0を公開
n点を検証、
属性秘密鍵s_{ij}を
暗号化

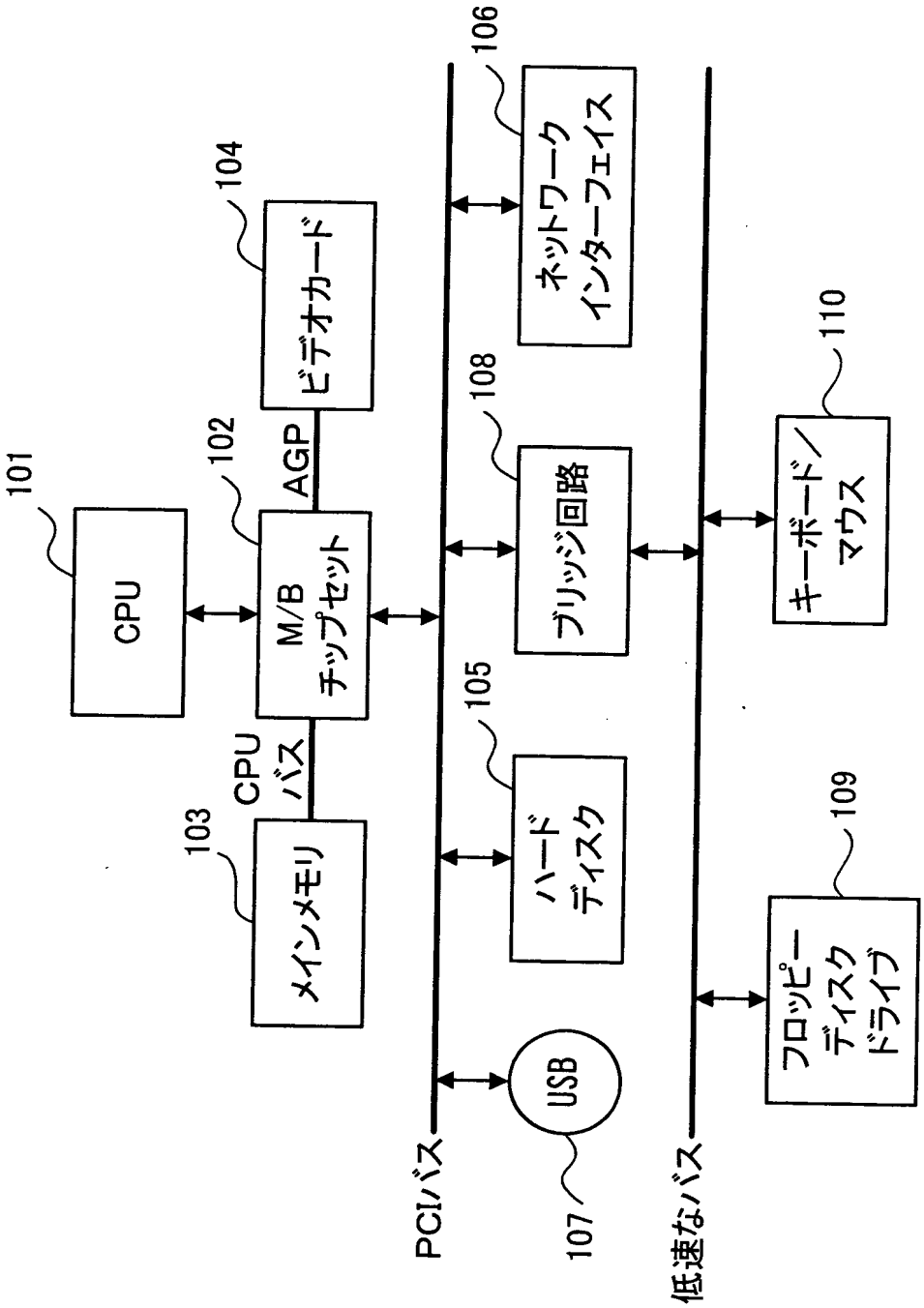
【図４】


条件鍵生成プロトコル
AND:
{E(yi0, Kij), E(yk1, Kkl)}
または
E(yi1, E(yk1, K))
OR:
{E(yi0, K), E(yk1, K)}
NOT:
E(yi1, K)||・・・||E(yij-1, K)||
E(yij+1, K)||・・・||E(yimi, K)
数値属性:
cj=E(sk(1)j, kj) if yj=1
cj=E(sk(0)j, K)||E(sk(1)j, kj)
if yj=0
など
公開鍵
条件鍵、
セッション鍵

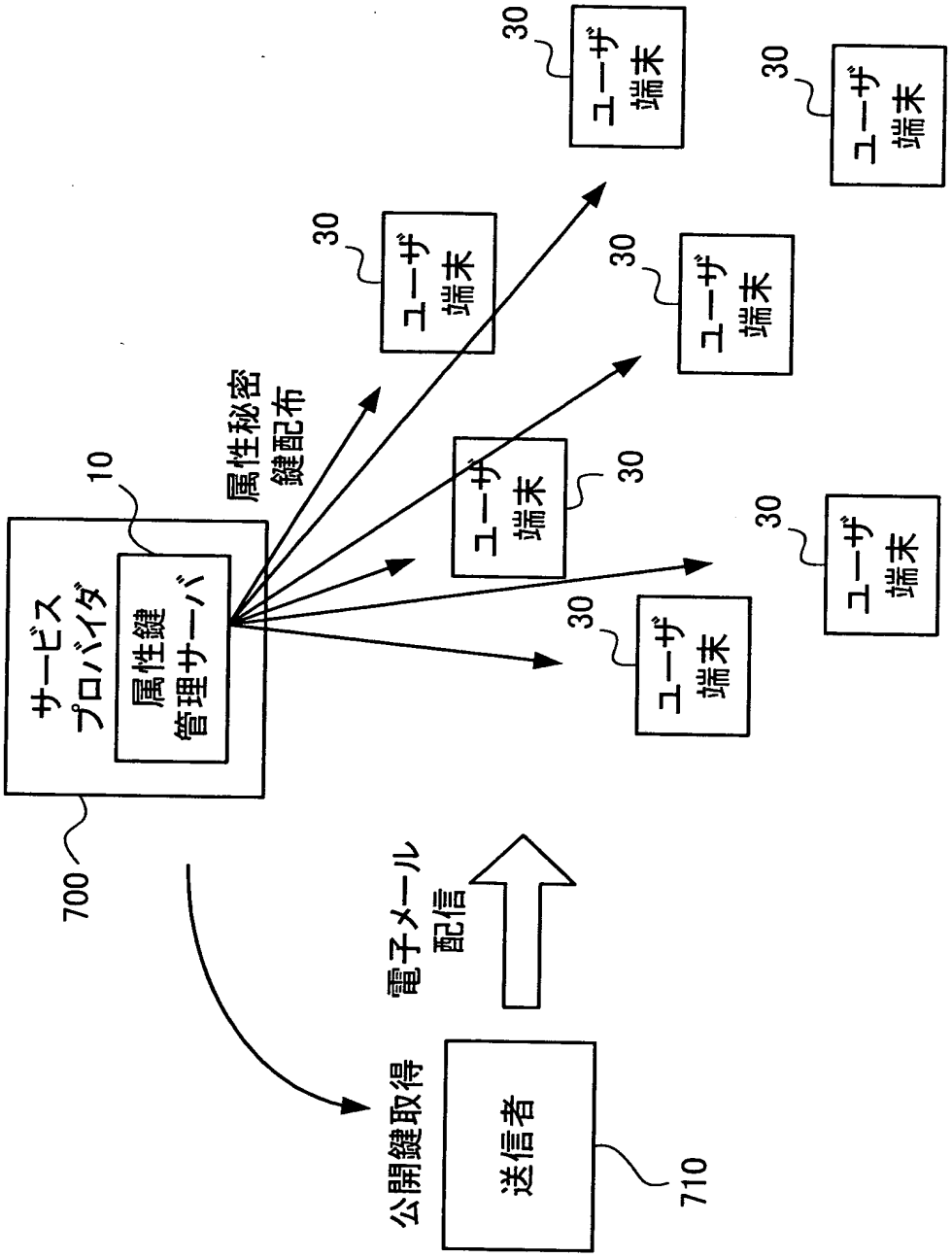
【図５】



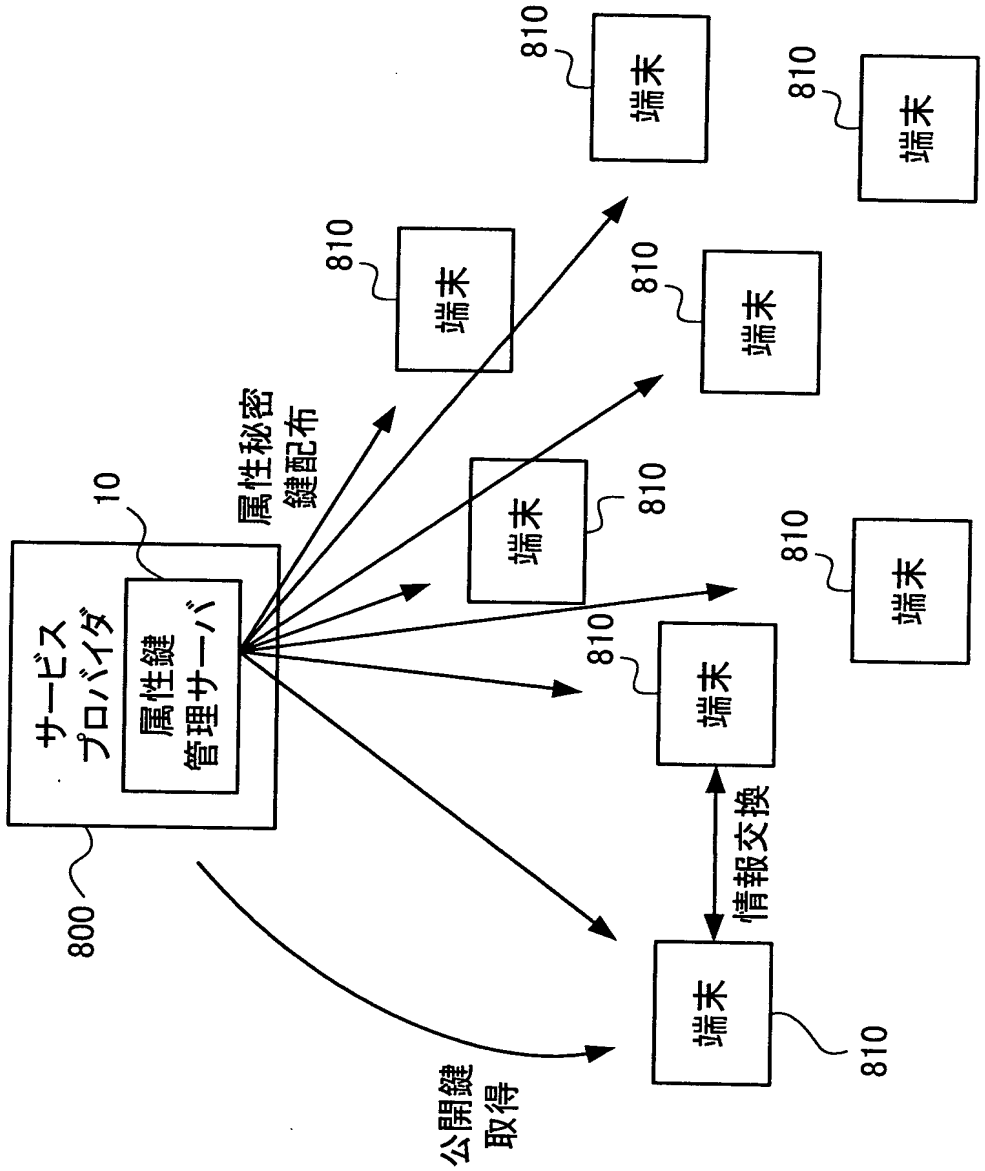
【図６】


101
CPU
102
M/B
チップセット
AGP
104
ビデオカード
CPU
バス
103
メインメモリ
106
ネットワーク
インターフェイス
108
ブリッジ回路
105
ハード
ディスク
USB
107
PCIバス
110
キーボード／
マウス
109
フロッピー
ディスク
ドライブ
低速なバス

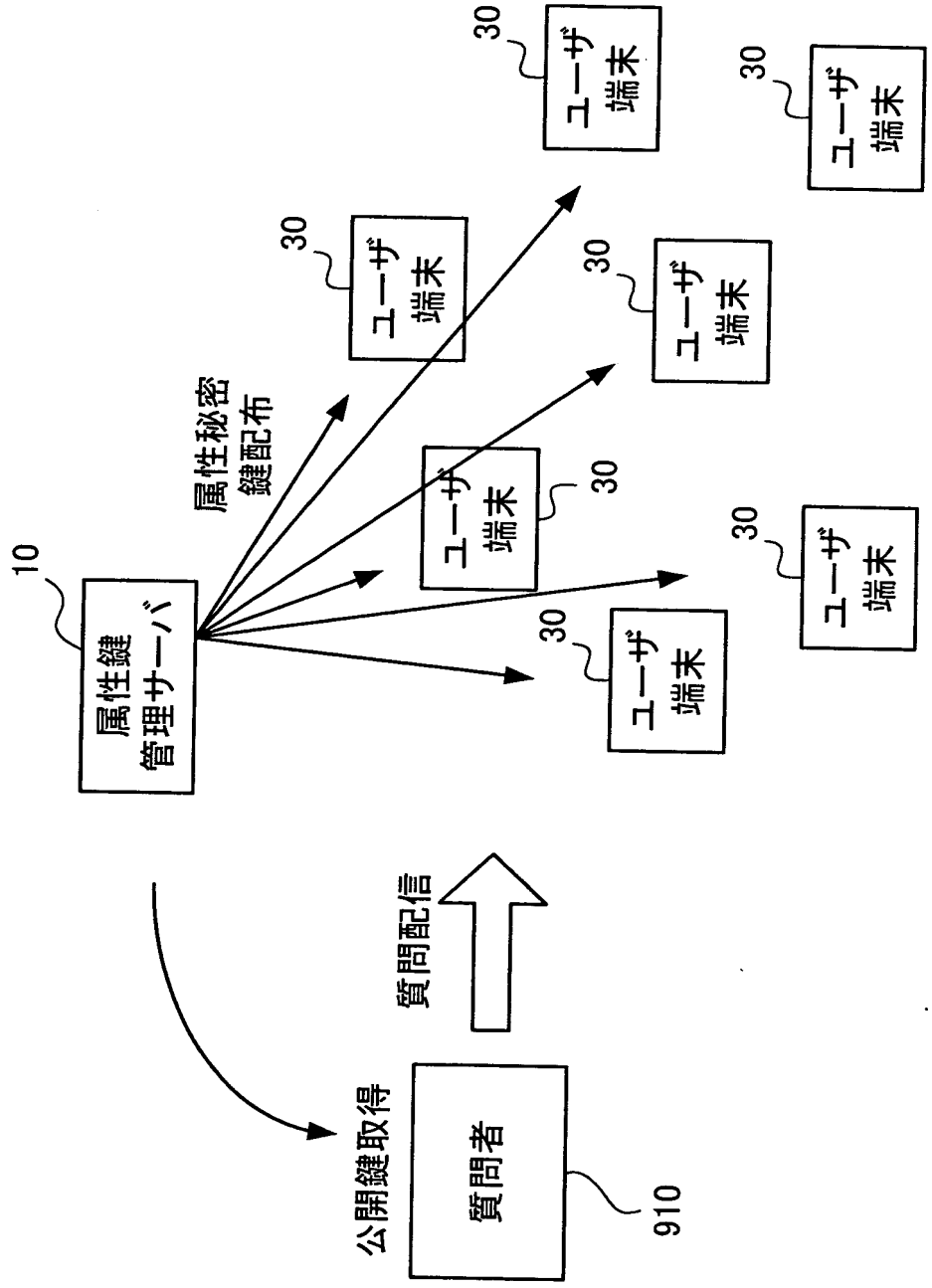
【図７】


サービス
プロバイダ
10
属性鍵
管理サーバ
700
属性秘密
鍵配布
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
電子メール
配信
公開鍵取得
送信者
710

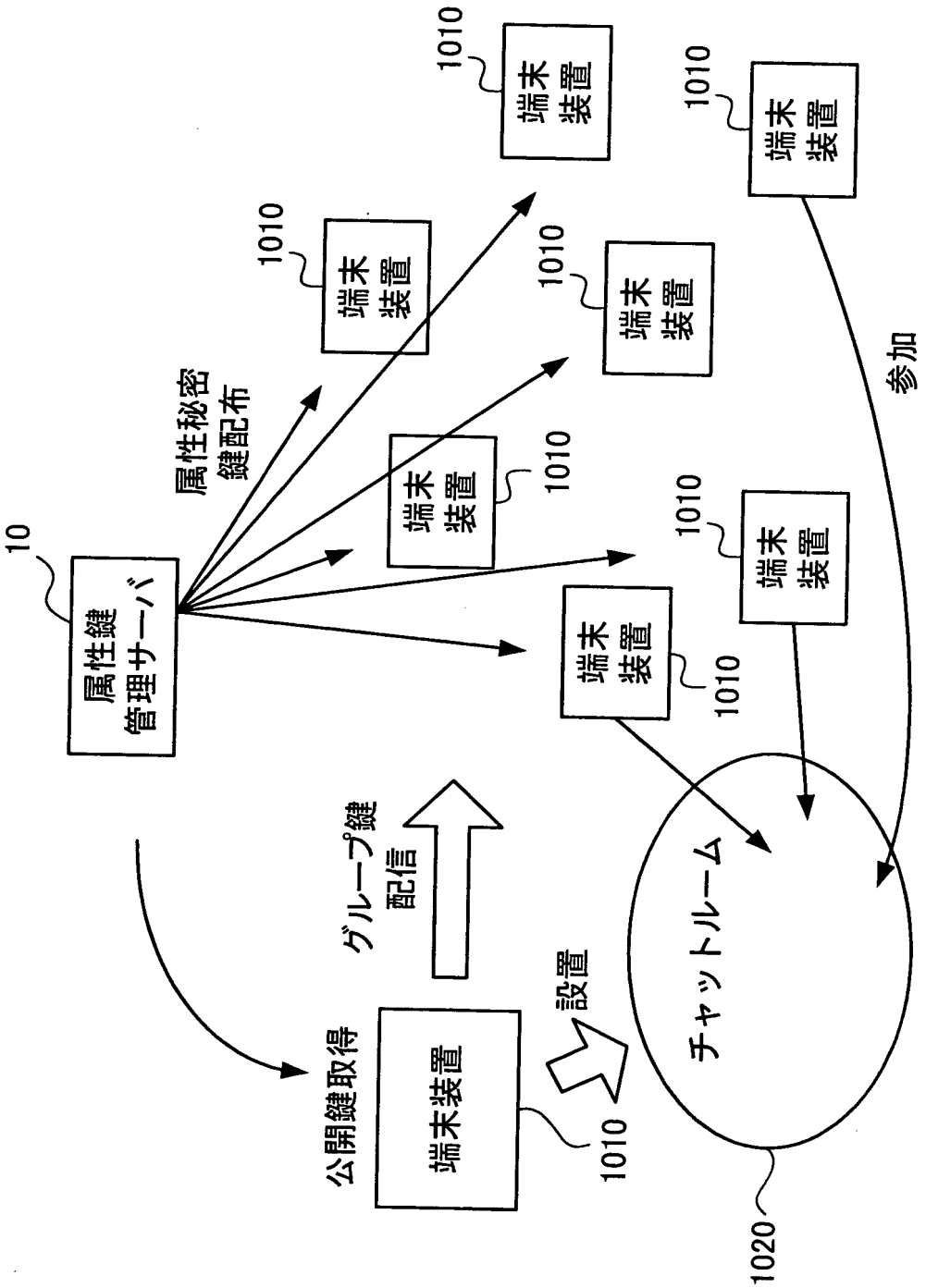
【図８】



【図９】


10
属性鍵
管理サーバ
属性秘密
鍵配布
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
30
ユーザ
端末
質問配信
公開鍵取得
質問者
910

【図１０】


10
属性鍵
管理サーバ
属性秘密
鍵配布
1010
端末
装置
参加
公開鍵取得
端末装置
設置
グループ鍵
配信
チャットルーム
1020

【書類名】　　要約書

【要約】

【課題】　受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を満たす人のみが受信できるような情報配信システムを提供する。

【解決手段】　所定の属性値に対する秘密鍵及び公開鍵を管理する属性鍵管理サーバ１０と、この属性鍵管理サーバ１０にアクセスし、秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得するユーザ端末３０と、公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末３０が復号可能な暗号化コンテンツを生成するプロバイダ端末２０とを備える。そして、このプロバイダ端末２０は、暗号化コンテンツを配信し、ユーザ端末３０は、自分の属性秘密鍵にて復号可能な暗号化コンテンツを復号する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００２－１８３５１１
受付番号	５０２００９２１４５６
書類名	特許願
担当官	末武　実　　１９１２
作成日	平成１４年　７月２３日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100106699

【住所又は居所】　東京都中央区日本橋本町３－１－１３　ロッツ和興ビル

【氏名又は名称】　渡部　弘道

【復代理人】　申請人

【識別番号】　100104880

【住所又は居所】　東京都港区赤坂５－４－１１　山口建設第２ビル６Ｆ　セリオ国際特許事務所

【氏名又は名称】　古部　次郎

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　２００２年　６月　３日
［変更理由］　住所変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション